قانون حماية البيانات الشخصية:
ما يمكن تَعلُّمه من تجارب الدول الأخرى

تشرين الثاني **2014**

شهد حموري | ريم المصري

مقدمة:

في أوائل عام 2014 قدمت وزارة الاتصالات الأردنية مشروعًا لقانون حماية البيانات الشخصية. قام أعضاء من فريق حبر – لاسلكي بالاشتراك مع عدة مؤسسات أخرى، بدراسة النص المقترح، وتقديم مقترحات لتطويره بناءً على الممارسات الدولية، ومراجع لقوانين في دول مختلفة. استنادًا لهذا البحث، حضّر فريق لاسلكي هذا الدليل البسيط الذي يقترح بعض الأسئلة والنقاط التي يمكن من خلالها قراءة ونقد أي مشروع مقدم لقانون حماية البيانات الشخصية وتقييم مدى فعاليته في حماية بيانات المواطنين.

أولًا: المفاهيم الواردة في قانون حماية البيانات واستثناءاته

1. تعريف البيانات الشخصية

البيانات الشخصية هي "أي معلومات خاصة بشخص طبيعي قابل للتعرف عليه" (انظر توجيه الأوروبي لحماية البيانات الشخصية). تكمن أهمية التعريف في توسيع نطاق حيز تطبيق القانون، إذ أن التضييق من مفهوم البيانات الشخصية قد يسمح للعديد من الجهات بالتعدي عليها. البيانات الموزعة بقواعد بيانات مختلفة قد لا تدل على هوية الشخص بحد ذاتها، لكن إذا تم ربطها قد تفصح عن هوية الشخص. بالتالي، في حال اكتفى النص بحماية البيانات التي ترتبط بصاحبها بشكل مباشر فقط، قد يسمح ذلك للعديد من الجهات بالتعدي على بيانات الأشخاص خاصة مع تقدم تقنيات جمع البيانات ومشاركتها.

- هل حدد المشرع مفهوم "قابل للتعرف عليه"؟
- هل وضع النص استثناءات عديدة على البيانات الشخصية التي يحميها القانون؟

2. تعريف البيانات الحساسة

البيانات المتعلقة بالعرق والديانة والمعتقدات والسجل الجرمي. تختلف خطورتها وأهميتها عن البيانات الأساسية مثل الأسم، تاريخ الميلاد والعنوان. إذ تتطلب بعض البيانات حماية أكبر من غيرها. مثلا يتطلب التوجيه الأوروبي من الجهة التي تنوي التعامل مع هذه البيانات الحساسة موافقة صاحب البيانات الصريحة (انظر أيضًا: قانون حماية البيانات البريطاني القسم الثاني).

- هل عدد النص أنواع البيانات الحساسة؟
- هل اشترط النص موافقة صريحة من صاحب البيانات لمعاجتها؟
- هل تختلف عقوبة استخدام البيانات الحساسة عن عقوبة اساءة استخدام البيانات العادية؟

ثانيًا: حقوق صاحب البيانات

3. الموافقة على عمليات البيانات

من أساسيات الحماية في قوانين حماية البيانات الشخصية هو حق صاحب البيانات بالموافقة على، أو رفض، أي من عمليات البيانات (الجمع ، المعالجة، المشاركة). قد يكتفي المشرع أحيانًا بالموافقة الضمنية، لكن التأكيد على الموافقة الصريحة يخدم مبدأ الشفافية أثناء التعامل مع البيانات (انظر المبدأ الثالث والمبدأ الخامس في مبادئ منتدى التعاون الأقتصادي لدول آسيا والمحيط الهادئ للخصوصية).

- ما عدد الحالات التي تتطلب الموافقة الصريحة، وهل اشترط التقيد بالحالات التي يوافق عليها صاحب البيانات فقط؟
- هل بالغت النصوص بالإجراءات الإدارية المطلوبة من الجهات التي تتعامل مع البيانات؟
- هل اشتُرط توفير سياسة خصوصية واضحة ومفهومة لصاحب البيانات؟

4. استثناءات اشتراط الموافقة

تتعامل الجهات الحكومية مع كميات كبيرة من البيانات، ومع ذلك قد تعفي نفسها من واجب حماية البيانات الشخصية في بعض الأحيان. فقد تجمع بيانات عن المواطنين بدون أي موافقة من قبلهم، أو تشارك بيانات المواطنين بين جهاتها المختلفة من دون مراعاة شروط عمليات البيانات (الجمع، المعالجة، المشاركة)، مخالفة بذلك أهم مبادئ حماية البيانات الشخصية للمواطنين. فالأصل هو عدم التفرقة بين النصوص التي تتعامل مع الجهات الجامعة الخاصة والجهات الحكومية، مع ذلك تقتضي طبيعة عمل الدولة بعض الاستثناءات عن القواعد الأصلية لحماية البيانات اثناء التعامل مع بيانات المواطنين (انظر الفصل 47 قانون حماية المعطيات التونسي)، ومثل كل الاستثناءات، لا بد أن تكون هذه الاستثناءات محدودة.

- هل حدد النص متى يسمح للجهات الحكومية بجمع، معالجة أو مشاركة بيانات المواطنين من دون موافقتهم؟
- من المصطلحات الفضفاضة المستخدمة من قبل الجهات الحكومية مصطلح "الأمن الوطني"، فهل وضع النص معايير واضحة لمفهوم "الأمن الوطني" أو أشار إلى قانون آخر يبحث بهذا المفهوم؟ (انظر مثال القانون الآيسلندي)[1].
- هل أشار النص إلى الجهات الحكومية ككل أم حدد الجهات الحكومية التي تستطيع أن تستثنى من التزام الحصول على موافقة صاحب البيانات قبل إجراء أي من عمليات البيانات؟

5. حق صاحب البيانات بالاطلاع على بياناته، وتعديلها، وتحديها

قد تخزن عنك جهة معينة كمية بيانات كبيرة لا علم لك بها، أو حتى بيانات غير صحيحة أحيانًا، لذا يستلزم مبدأ شفافية التعامل بين صاحب البيانات والجهة التي تتعامل بها، ومبدأ الحفاظ على دقة البيانات (انظر مبادئ الخصوصية في منظمة التعاون الاقتصادي والتنمية مبدأ 7) السماح لصاحب البيانات بالاطلاع على بيانته وتعديلها.(ما أسماه المشرع التونسي بحق النفاذ).

- هل أعطى النص صاحب البيانات حق الاطلاع على البيانات المتعلقة به وتعديلها؟
- هل ألزم النص الجهة الجامعة للبيانات بتوفير وسائل عملية يستطيع من خلالها الاطلاع على بياناتك وتعديلها؟

ثالثًا: التزامات الجهة التي تتعامل مع البيانات

6. عند مشاركة البيانات بين الجهات

تلجأ العديد من الجهات إلى مشاركة البيانات بينها إما للتعاون بغاية تقديم خدمات لصاحب البيانات أو لأهداف ربحية. ينطوي على هذه المشاركة مخاطر عديدة على بياناتك الشخصية خاصة مع تزايد المشاركة الإلكترونية بين الجهات المختلفة. لا بد من أن تلتزم هذه الجهات بإخطار لجنة حماية البيانات عن هذه المشاركة، وأهدافها ووسائلها (انظر تعليمات حماية البيانات الصادرة عن لجنة حماية البيانات البريطانية)، وعلى لجنة حماية البيانات مراقبة تعامل هذه الجهات مع البيانات.

- هل اشترط النص تبليغ اللجنة بهذه المشاركة بين الجهات المختلفة؟
- هل اشترط إيضاح أسباب ووسائل المشاركة بين الجهات بشكل مفصل لكل من اللجنة وصاحب البيانات؟

7. مشاركة البيانات عبر الحدود

تمتاز مشاركة البيانات عبر الحدود بقواعد خاصة بها. إذ لا يستطيع القانون المحلي حماية البيانات بعد خروجها من الدولة، خاصة مع انتشار الوسائل الاكترونية لتخزين البيانات مثل الحوسبة السحابية (Cloud Computing) مما قد يسمح للعديد من الانتهاكات لهذه البيانات في الدولة المستقبلة للبيانات.

- هل اشترط النص الموافقة الصريحة الخاصة لمشاركة البيانات عبر الحدود؟
- هل اشترط النص إجراءات أمنية خاصة مثل التشفير لحماية البيانات أثناء مشاركتها؟
- هل اشترط النص نقل البيانات فقط إلى الدول التي توفر مستوى مماثل من حماية البيانات (راجع معايير إعتماد قانون حماية البيانات في التوجيه الأوروبي).

[1] عدد القانون الآيسلندي مفاهيم أمن الدولة والدفاع في قانون العقوبات وأشار إليه في قانون حماية البيانات.

8. الحد من مدة احتجاز البيانات

بقاء البيانات مخزنة طويلًا لدى الجهة التي تعالج البيانات يسمح لهذه الجهة باعادة استخدامها، ويزيد من المخاطر التي قد تتعرض لها بياناتك، فمثلًا عندما تغلق حسابك على فيسبوك تبقى بياناتك مؤرشفة لديهم. في نفس الوقت، هناك جهات تخزن بيانات عنك مثل شركات الاتصالات.

- هل حدد النص مدة تلتزم بعدها الجهة بحذف البيانات التي تخص شخص معين؟
- هل أعطى النص صاحب البيانات حق حذف بياناته؟

رابعًا: وسائل تنفيذ القانون

9. تشكيل مجلس الخصوصية

حتى تطبق هذه القواعد لا بد من وجود هيئة تنفيذية تراقب عمليات البيانات، وعند نشوب نزاع لا بد من تشكيل لجنة تفصل في هذه النزاعات حول عمليات البيانات. يجب أن تتسم لجنة بالاستقلالية والحرفية حتى تستطيع النظر في النزاعات التي تنشب عن عمليات البيانات، بالتالي تكون آلية اختيار الأعضاء تضمن استقلال هذه الهيئة، ولدى هؤلاء الأعضاء خلفيات معينة تسمح لهم ممارسة دورهم في اللجنة.

- هل آلية تشكيل اللجنة تضمن استقلاليتها (انظر القانون الآيسلندي لحماية البيانات مادة 36)[2]؟
- هل يشترط النص ضم متخصصين قانونين وتقنيين ذوي خبرة في مجال حماية البيانات الشخصية إلى الهيئة؟
- هل تسمح النصوص لصاحب البيانات أو الجهة بالعودة إلى المحاكم في الحالات التي لا تختص فيها اللجنة، أو لاستئناف قرارتها؟

10. الاحتياطات الأمنية

حماية البيانات من أي أختراق خلال عمليات جمعها أو معالجتها أو مشاركتها هو واجب على الجهة جامعة البيانات. على هيئة حماية البيانات التأكد من وجود هذه الاحتياطات وفعاليتها (انظر قانون كوريا الجنوبية لحماية البيانات).[3] في ذات الوقت، قد تحاول بعض الجهات أحيانًا الإفلات من مسؤوليتها عند حدوث أي خرق للبيانات مثل العديد من الجهات الدولية التي تعرضت لخروقات أمنية ولا بد من أن يمنع النص هذه الجهات من التهرب من المسؤولية في حال نتج هذا الخرق عن إهمال منها.

- هل اشتُرط على الجهة أخذ تدابير مشددة لحماية البيانات؟
- هل يحق لصاحب البيانات المطالبة بالتعويض في حال تم الكشف عن البيانات أو فقدانها بسبب إهمال الجهة الجامعة لها؟

11. آلية الاخطار

لكي تمارس هيئة حماية البيانات وظيفتها في مراقبة عمليات البيانات، لا بد من أن يكون لديها علم بأسماء الجهات التي تتعامل بالبيانات الشخصية، بالإضافة إلى طبيعة عمليات البيانات التي تقوم بها ومبررات هذه العمليات. يتم ذلك من خلال علمية إخطار/تسجيل لدى هيئة حماية البيانات الشخصية. لكن قد ينطوي هذا الاخطار على كم كبير من الإجراءات الإدارية على الجهة جامعة البيانات، وقد يكون هناك جهات تتعامل بكمية صغيرة من البيانات الشخصية لا تستوجب مثل هذا الإخطار.

- هل ذُكر بدقة ما هي البيانات التي يجب أن ترد في التسجيل-الإخطار؟
- هل حدد النص متى يجب على الجهة الإخطار (هل اشتُرط الإخطار عند القيام بأي تعديل على سياسة الخصوصية أم الإخطار الدوري كل عدة سنوات مثلاً ؟
- هل حدد النص الجهات المستثنية من الإخطار؟ (راجع القانون الإيرلاندي لحماية البيانات الشخصية).

---

[2] ينص القانون الآيسلندي على أن يتم تعين الأعضاء من قبل الرئيس، إلا أن الأعضاء الخمسة يتم تعيينهم كل أربع سنوات. الأعضاء: رئيس المجلس ونائب الرئيس لا يحتاجون لأي ترشيح من أي جهة ويشترط فيهم أن يكونوا محامين مؤهلين لمنصب قضاة. وعضو ترشحه المحكمة العليا وعضو يرشحه المجتمع الآيسلندي لمعالجة المعلومات ويشترط كونه ضليعًا في مجال التكنولوجيا.

[3] مثلًا: يشترط القانون الكوري لحماية البيانات 2011 اتباع وسائل محددة ومعينة من قبل التعليمات الصادرة من وزارة الاتصالات في حماية البيانات، وشدد على الوسائل المتبعة في حالات معينة مثل نقل البيانات عبر الحدود، وتخضع هذه الوسائل لتفتيش من قبل خبراء. بالإضافة إلى ذلك، أناط القانون بهيئة حماية البيانات دورًا توعويًا بنشر معلومات عن طرق حماية البيانات بين الأفراد.